



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

10/600,683

06/20/2003

Erik Olson

13768.373

4994

47973

7590

07/21/2006

WORKMAN NYDEGGER/MICROSOFT
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UT 84111

EXAMINER

WILLIAMS, JEFFERY L

ART UNIT

PAPER NUMBER

2137

DATE MAILED: 07/21/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

10/600,683

Applicant(s)

OLSON ET AL.

Examiner

Jeffery Williams

Art Unit

2137

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 25 April 2006.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-25 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-25 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☒ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 20 June 2003 is/are: a) ☐ accepted or b) ☒ objected to by the Examiner.
- Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: _____.

DETAILED ACTION

Claims 1 – 25 are pending.

This action is in response to the communication filed on 4/25/2006.

All objections and rejections not set forth below have been withdrawn.

Drawings

Figures 1 should be designated by a legend such as --Prior Art-- because only that which is old is illustrated. See MPEP § 608.02(g). Corrected drawings in compliance with 37 CFR 1.121(d) are required in reply to the Office action to avoid abandonment of the application. The replacement sheet(s) should be labeled "Replacement Sheet" in the page header (as per 37 CFR 1.84(c)) so as not to obstruct any portion of the drawing figures. If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

Specification

The specification is objected to as failing to provide proper antecedent basis for the claimed subject matter. See 37 CFR 1.75(d)(1) and MPEP § 608.01(o). Correction of the following is required:

The specification does not provide antecedent basis for the added limitations of claims 1 – 25 for *“requesting that the user computer resubmit the request and subsequently executing the resubmitted request only upon determining that it does not contain the marker of active content”*.

Claim Rejections - 35 USC § 112

The following is a quotation of the first paragraph of 35 U.S.C. 112:

The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

Claims 1 – 25 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the

1 **time the application was filed, had possession of the claimed invention. See**
2 **above objection to the specification.**

3
4 The following is a quotation of the second paragraph of 35 U.S.C. 112:

5 The specification shall conclude with one or more claims particularly pointing out and distinctly
6 claiming the subject matter which the applicant regards as his invention.

7
8 **Claims 1 – 25 are rejected under 35 U.S.C. 112, second paragraph, as being**
9 **indefinite for failing to particularly point out and distinctly claim the subject**
10 **matter which applicant regards as the invention.**

11 Claims 1, 8, and 18 each recite the limitation "the resubmitted request" (i.e. claim
12 1, line 13). There is insufficient antecedent basis for this limitation in the claims, as the
13 claims do not provide the limitation that a request has been resubmitted. For the
14 purposes of examination, the examiner will presume the applicant to refer to "a
15 resubmitted request".

16
17 All other claims are rejected by virtue of dependency.

18
19
20 ***Claim Rejections - 35 USC § 103***

21
22 The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all
23 obviousness rejections set forth in this Office action:

24 (a) A patent may not be obtained though the invention is not identically disclosed or described as set
25 forth in section 102 of this title, if the differences between the subject matter sought to be patented and

Art Unit: 2137

1 the prior art are such that the subject matter as a whole would have been obvious at the time the
2 invention was made to a person having ordinary skill in the art to which said subject matter pertains.
3 Patentability shall not be negated by the manner in which the invention was made.
4

5 **Claims 1 – 6, 8 – 13, 15 – 23, and 25 are rejected under 35 U.S.C. 103(a) as**
6 **being unpatentable over CERT CC, “CERT Advisory CA-2000-02 Malicious HTML**
7 **Tags Embedded in Client Web Requests” (CERT-Advisory) in view of CERT CC,**
8 **“Understanding Malicious Content Mitigation for Web Developers” (CERT) in view**
9 **of Hidalgo et al. (Hidalgo), “Firewalls for Providing Security in Http Networks and**
10 **Applications”, U.S. Patent 2002/0051142 in view of Fielding et al. (Fielding),**
11 **“Hypertext Transfer Protocol – HTTP/1.1”, RFC 2616.**
12

13 Regarding claim 8, CERT-Advisory discloses:

14 *receiving an HTTP request at a server computer, wherein the HTTP request*
15 *includes input data that was not generated by the server computer (CERT-Advisory,*
16 *page 1, Systems Affected, Overview; page 2, pars. 2-4).*

17 CERT-Advisory discloses, in general, that the Server site attempts to filter the
18 incoming HTTP request according to the criteria of removing dangerous meta-
19 characters, so as to prevent their sites from being attacked, “abused”, by malicious data
20 or a cross-site scripting attack (CERT-Advisory, page 5, Solutions for Web Page
21 Developers and Web Site Administrators). While one of ordinary skill in the art would
22 rightly and easily conclude from the context of CERT-Advisory that the incoming meta-
23 characters being filtered are being evaluated against known scripting constructs or
24 characters, CERT-Advisory does not *explicitly* say the evaluation is to determine *if the*
25 *input data includes a script construct, wherein the script construct indicates that HTTP*

1 *request is part of a cross-site scripting attack.* Instead, CERT-Advisory directs the
2 readers' attention to the detailed solution (found in CERT) for preventing cross-site
3 scripting attacks in response to receiving HTTP requests comprising malicious scripts.

4 CERT discloses the specifics for mitigating cross-site scripting attacks by
5 evaluating the incoming data requests to determine the presences of dangerous meta-
6 characters, indicating the presence of malicious scripts (CERT, page 1, par. 1, Problem
7 Summary, pars. 2-3; page 2, Mitigation Summary; page 3, Identifying the Special
8 Characters; page 4, Filtering Dynamic Content). CERT, thus clearly demonstrates that
9 the filtering of input data for dangerous meta-characters is an evaluation of the
10 presence of malicious script constructs.

11 It would have been obvious to one of ordinary skill in the art to combine the
12 teachings of CERT, for evaluating input data for script constructs - in addition to other
13 specific teachings of CERT for mitigating cross-site scripting attacks - with the system of
14 CERT-Advisory. This would have been obvious because CERT-Advisory explicitly says
15 to include the reference of CERT so as to successfully mitigate cross-site scripting
16 attacks (CERT-Advisory, page 5, par. 6).

17 The combination of CERT-Advisory and CERT discloses *refusing to execute*
18 *HTTP request and thereby preventing the cross-site scripting attack if the input data*
19 *includes a script construct* (CERT-Advisory, pg. 1, "Overview"; pg. 2, "Malicious code
20 sent inadvertently by a client for itself"; CERT, pg. 1, par. 1; pg. 2-4, "Mitigation
21 Summary"). Herein, the combination shows that malicious HTTP requests are not
22 executed. Furthermore, the combination discloses filtering and encoding to remove

1 malicious scripts and data for every HTTP request. That which is subsequently
2 executed is not the original malicious request. Thus, the combination teaches
3 *subsequently executing the resubmitted HTTP request only upon determining that it*
4 *does not contain the script construct* (note that any ["resubmitted"] malicious request is
5 not executed).

6 The combination of CERT-Advisory and CERT discloses a system for mitigating
7 cross-site scripting attacks by evaluating the incoming HTTP data requests to determine
8 the presence of a malicious script. The combination does not disclose informing the
9 user computer that a marker of active content has been discovered in the request,
10 namely *generating a response indicating that a script construct indicative of a cross-site*
11 *scripting attack has been received.*

12 Hidalgo also discloses a system for mitigating cross-site scripting attacks that
13 stem from invalid HTTP requests (Hidalgo, par. 14, 58-66). Hidalgo teaches that when
14 invalid HTTP requests are discovered, a system can send an informative error alert to
15 the user that sent the invalid request.

16 It would have been obvious to one of ordinary skill in the art to combine the
17 teachings of Hidalgo within the combination of CERT-Advisory and CERT. This would
18 have been obvious because one of ordinary skill in the art would have been motivated
19 by inform users of danger or possible malicious activity and thus create a more user-
20 friendly and informative system.

21 The combination of CERT-Advisory, CERT, and Hidalgo discloses the sending of
22 an error to the user to inform the user that an invalid HTTP request has been received.

1 The combination also teaches that information regarding malicious content enables one
2 to recognize attacks and take proactive measures (CERT, pg. 1, "Problem Summary",
3 par. 1). The combination, however, does not disclose providing information that would
4 request *resubmission of the HTTP request*.

5 Fielding discloses that error messages for invalid HTTP requests indicate that an
6 error has occurred on the user side (Fielding, pg. 65, sect. 10.4). Fielding discloses
7 that such error messages will inform that resubmitted requests should be corrected
8 (Fielding, pg. 65, sect. 10.4.1) or be used in situations where the user is expected to
9 take corrective measures and resubmit the request (Fielding, pg. 67, sect. 10.4.10).

10 It would have been obvious to one of ordinary skill in the art to incorporate the
11 teachings of Fielding within the error messages of the combination of CERT-Advisory,
12 CERT, and Hidalgo, and thus provide information to the user that a resubmitted HTTP
13 request is desired. This would have been obvious because one of ordinary skill in the
14 art would have been motivated to allow a user to learn and take proactive measures to
15 ensure the safety of his/her communications. For example, a user could be informed
16 that his HTTP request, which was submitted by clicking on a link, was invalid or
17 malicious and would be encouraged to safely resubmit a subsequent request, such as
18 by manually keying in the correct URL.

19
20 Regarding claim 9, the combination of CERT-Advisory, CERT, Hidalgo, and
21 Fielding disclose:

1 *at least one of: receiving a query string that includes at least one query string*
2 *variable; receiving a cookie; receiving one or more headers in the HTTP request; and*
3 *receiving one or more form fields (CERT-Advisory, page 2, pars. 2-5; CERT, page 2,*
4 *Mitigation Summary).*

5
6 Regarding claim 10, the combination of CERT-Advisory, CERT, Hidalgo, and
7 Fielding disclose:

8 *at least one of: searching the HTTP request for one or more character*
9 *combinations that correspond to a script construct; searching the HTTP request for an*
10 *event that includes a script construct; searching server variables that derive input data*
11 *from another source; and searching the HTTP request for an expression that includes a*
12 *script construct (CERT, page 3, Identifying the Special Characters; page 4, Filtering*
13 *Dynamic Content).*

14
15 Regarding claim 11, the combination of CERT-Advisory, CERT, Hidalgo, and
16 Fielding disclose:

17 *searching the input data for a script construct (CERT, page 3, Identifying the*
18 *Special Characters; page 4, Filtering Dynamic Content).*

19
20 Regarding claim 12, the combination of CERT-Advisory, CERT, Hidalgo, and
21 Fielding disclose:

1 *searching for patterns associated with scripts* (CERT, page 3, Identifying the
2 Special Characters; page 4, Filtering Dynamic Content).

3
4 Regarding claim 13, the combination of CERT-Advisory, CERT, Hidalgo, and
5 Fielding disclose:

6 *refraining from executing the HTTP request* (CERT-Advisory, page 2, par. 1;
7 page 5, pars. 3-6). In addition to plainly refraining from executing a compromised HTTP
8 request, CERT-Advisory also discloses the filtering and/or recoding of a compromised
9 request into a well-formed HTTP request, thus refraining from executing the
10 compromised HTTP request.

11
12 Regarding claim 15, the combination of CERT-Advisory, CERT, Hidalgo, and
13 Fielding disclose:

14 *encoding the user input including the script construct to render the script inert*
15 (CERT-Advisory, page 2, par. 1; page 5, pars. 3-6; CERT, page 3, Identifying the
16 Special Characters; page 4, par. 2).

17
18 Regarding claim 16, the combination of CERT-Advisory, CERT, Hidalgo, and
19 Fielding disclose:

20 *evaluating the HTTP request to determine in the input data includes a marker of*
21 *active content* (CERT, page 2, Mitigation Summary – particularly steps 2 and 4; page 3,
22 Identifying the Special Characters).

Regarding claim 17, the combination of CERT-Advisory, CERT, Hidalgo, and Fielding disclose:

determining if the marker of active content is within a particular element, wherein the marker of active content is harmful only when rendered within the particular element (CERT, page 2, Mitigation Summary – particularly steps 2 and 4 (identifying special characters, filtering specific characters in dynamic elements; page 3, Identifying the Special Characters).

Regarding claims 1 – 3, 5, 6, 18 – 23, and 25, they are method and method embodied on computer readable medium claims corresponding to the system claims 1 – 17, and they are rejected, at least, for the same reasons.

Regarding claim 4, the combination of CERT-Advisory, CERT, Hidalgo, and Fielding disclose: *evaluating only a portion of the request that includes the data derived from an outside source* (CERT, page 2, Mitigation Summary). The combination of CERT-Advisory and CERT discloses the need to evaluate data comprising untrusted input that could be transmitted in an HTTP request.

Claims 7, 14, and 24 are rejected under 35 U.S.C. 103(a) as being unpatentable over the combination of CERT-Advisory, CERT, Hidalgo, and

**Fielding in view of Fischman et al. (Fischman), U.S. Patent Publication
2003/0097588.**

Regarding claim 14, the combination of CERT-Advisory and CERT does not disclose the logging of attacks to the system. Namely, the combination of CERT-Advisory and CERT does not disclose *wherein preventing the cross-site scripting attack if the input data includes a script construct further comprises logging an event at the server computer.*

Fischman discloses a method wherein attacks to the security of a server system are logged. This allows the operators of the system to access the log and become aware of problems and to make proper adjustments if necessary (Fischman, par. 45).

It would be obvious to one of ordinary skill in the art to employ the method of Fischman for logging system attacks within the system of the combination of CERT-Advisory and CERT. This would have been obvious, because one of ordinary skill in the art would have been motivated to provide the proactive benefits of logging taught by Fischman to the operators of the attacked web server of the combination CERT-Advisory and CERT, thus enabling the server operators to access a an attack log and make system improvements.

Response to Arguments

Applicant's arguments filed 4/25/06 have been fully considered but they are not persuasive.

Applicant's arguments with respect to claims 1 - 25 have been considered but are moot in view of the new ground(s) of rejection.

Applicant's argue primarily that:

(i). *For example, Figure 1 illustrates a block diagram of a network environment in which an electronic message may be used in facilitating a cross-scripting attack of a "Hello" HTML page returned from a server to a user computer. The displayed user computer and server can also be construed to include the inventive modules and computer-executable instructions described throughout the application (although they are not explicitly referenced in Figure 1). Nevertheless one of skill in the art would recognize their presence in view of the disclosure of the application. (Remarks, pg. 11 – applicants' reason for the traversal of the objection to drawing 1)*

In response, the examiner respectfully points out that figure 1 is Prior Art, as figure 1 illustrates only that which was known.

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure:

See Notice of References Cited

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than **SIX MONTHS** from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jeffery Williams whose telephone number is (571) 272-7965. The examiner can normally be reached on 8:30-5:00.

Art Unit: 2137

1 If attempts to reach the examiner by telephone are unsuccessful, the examiner's
2 supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone
3 number for the organization where this application or proceeding is assigned is 571-
4 273-8300.

5 Information regarding the status of an application may be obtained from the
6 Patent Application Information Retrieval (PAIR) system. Status information for
7 published applications may be obtained from either Private PAIR or Public PAIR.
8 Status information for unpublished applications is available through Private PAIR only.
9 For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should
10 you have questions on access to the Private PAIR system, contact the Electronic
11 Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a
12 USPTO Customer Service Representative or access to the automated information
13 system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

14
15
16 J. Williams
17 AU: 2137

18 JW
19

Jacqueline
JACQUES LOUIS JACQUES
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100